Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 346 (2005) 113–134
Theoretical Computer Science
www.elsevier.com/locate/tcs

On finite-state approximants for probabilistic computation tree logic

Michael Huth*

Department of Computing, Imperial College London, London SW7 2AZ, UK

Abstract

We generalize the familiar semantics for probabilistic computation tree logic from finite-state to infinite-state labelled Markov chains such that formulas are interpreted as measurable sets. Then we show how to synthesize finite-state abstractions which are sound for full probabilistic computation tree logic and in which measures are approximated by monotone set functions. This synthesis of sound finite-state approximants also applies to finite-state systems and is a probabilistic analogue of predicate abstraction. Sufficient and always realizable conditions are identified for obtaining optimal such abstractions for probabilistic propositional modal logic.

Keywords: Markov chain; Probabilistic model checking; Abstraction; Optimality

1. Introduction

Probabilistic model checking has high complexity in the size of finite models [7] and some models are infinite, perhaps with uncountable state space. It is therefore important to develop abstraction techniques so that verifications and refutations of probabilistic behavior can be carried out on abstract models and transferred to the models they abstract.

This paper proposes such a technique for the general class of labelled Markov chains, whose state spaces are sets of any size but endowed with the measure-theoretic structure of a σ-algebra and a stochastic kernel [15]. We generalize a semantics for Hansson and Jonsson's probabilistic computation tree logic [22] (PCTL) to such models and prove that

* Tel.: +44 20 7594 8244; fax: +44 20 7581 8024.
E-mail address: M.Huth@doc.imperial.ac.uk.

0304-3975/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2005.08.008

this semantics is well defined, which amounts to showing that the set of states satisfying a given formula is measurable. Then we adapt techniques from qualitative abstraction (see e.g. [21]) to the synthesis of finite-state approximants for such models. Each approximant constructed in this way carries may- and must-structure and is proved to be sound with respect to the semantics on the concrete model. May-structure takes an optimistic view of the concrete system whereas must-structure abstracts the concrete system pessimistically [9]. Formulas of PCTL are therefore interpreted on may- or must-structure depending on their logical polarities.

Furthermore, we adapt the techniques of Danos and Desharnais for proving optimality results [12] to deal with a probabilistic logic with negation. Specifically we prove that, under mild and always realizable restrictions, for any finite set of formulas of PCTL without the temporal operator "Until" and concrete model there is a finite-state approximant whose model checks for these formula are the same as those on the concrete model.

Outline of this paper: In Section 2 we recall required concepts from measure theory. Section 3 features the models and their semantics for PCTL without the temporal operator "Until" and shows that this semantics is well defined. The systematic construction of sound finite-state, even optimal, approximants for such models and formulas is the topic of Section 4. The concrete semantics for full PCTL is defined in Section 5 and its abstract semantics is presented and shown to be sound in Section 6. Section 7 states related work, Section 8 sketches future work, and Section 9 concludes.

2. Concepts from measure theory

We define needed concepts from measure theory (see e.g. [4]). We write $\mathbb{N} = \{0, 1, 2, \ldots\}$ for the set of natural numbers. A σ-algebra Σ on a set S is a subset of $\mathbb{P}(S)$, the powerset of S, that contains S and is closed under set complements $A \mapsto S \setminus A : \Sigma \to \Sigma$ and countable unions: $\{A_n \mid n \in \mathbb{N}\} \subseteq \Sigma$ implies $\bigcup_{n\in\mathbb{N}} A_n \in \Sigma$. We then call (S, Σ) a measure space. Given any $\Theta \subseteq \mathbb{P}(S)$, there is a smallest σ-algebra containing Θ, the σ-algebra generated by Θ in S. Let B be the Borel algebra, the σ-algebra on the unit interval of real numbers $[0, 1]$ generated by all intervals in $[0, 1]$. A finite measure μ on a measure space (S, Σ) is a function $\mu : \Sigma \to [0, r]$ with $r < \infty$ such that μ is σ-additive: for all countable collections $(A_n)_{n\in\mathbb{N}}$ of pairwise disjoint elements of Σ we have $\mu(\bigcup_{n\in\mathbb{N}} A_n) = \sum_{n\in\mathbb{N}} \mu(A_n)$. We call $\mu(S)$ the mass of μ. Such a finite measure is a probability (sub-probability) measure if $\mu(S) = 1$ ($\mu(S) \leqslant 1$, respectively). For $s \in S$ the Dirac measure $\delta_s : \Sigma \to [0, 1]$ is the probability measure that maps each $A \in \Sigma$ with $s \in A$ to 1 and all other $A \in \Sigma$ to 0. If $\mu : \Sigma \to [0, r]$ is a finite measure, its inner (μ_*) and outer measure (μ^*) both have type $\mathbb{P}(S) \to [0, r]$, are defined as $\mu_*(A) = sup\{\mu(X) \mid A \supseteq X \in \Sigma\}$ and $\mu^*(A) = inf\{\mu(X) \mid A \subseteq X \in \Sigma\}$, are monotone (as $A \subseteq A'$ implies $\mu_*(A) \leqslant \mu_*(A')$ and $\mu^*(A) \leqslant \mu^*(A')$), are not ($\sigma$-)additive in general, but satisfy $\mu_*(A) \leqslant \mu^*(A)$ for all $A \subseteq \mathbb{P}(S)$. A function $f : \Sigma \to \mathsf{B}$ is measurable iff for all $B \in \mathsf{B}$, $f^{-1}(B) \in \Sigma$; we then abuse notation and write

$$f : (S, \Sigma) \to ([0, 1], \mathsf{B}) .$$

If f and g are measurable, then so are $\max(f, g)$ and $\min(f, g)$ where these operations apply point-wise. Given $A \subseteq S$ we write $\chi_A : S \to [0, 1]$ for the function which maps all $s \in A$ to

1 and all other $s \in S \setminus A$ to 0. If $A \in \Sigma$, then $\chi_A : (S, \Sigma) \to ([0,1], \mathsf{B})$ is measurable. Given a measure space (S, Σ), a stochastic kernel k on (S, Σ) is a function $k : S \times \Sigma \to [0,1]$ such that, for all $s \in S$, the function $\lambda A.k(s, A) : \Sigma \to [0,1]$ is a sub-probability measure and, for all $A \in \Sigma$, the function $\lambda s.k(s, A) : (S, \Sigma) \to ([0,1], \mathsf{B})$ is measurable. We refer to [4] for a primer on integration theory but state all relevant facts about integration over finite measures in proofs.

3. Probabilistic modal logic for labelled Markov chains

The notion of model we use for probabilistic systems, labelled Markov chains, is familiar from the theory of random processes. Labelled Markov chains are state-based analogues of Desharnais et al.'s labelled Markov processes [17,18]. Throughout this paper, AP denotes a set of atomic propositions.

Definition 1. A *labelled Markov chain* M is a tuple (S, Σ, R, L), where S is a set of states—whose cardinality is unrestricted—Σ is a σ-algebra on S, $R : S \times \Sigma \to [0,1]$ is a stochastic kernel, and $L : \mathsf{AP} \to \Sigma$ is a labelling function for atomic propositions $q \in \mathsf{AP}$ so that $L(q)$ denotes the set of states s at which q holds.

The results of this paper also apply to models with finite measures with a uniform bound $r < \infty$, where $\mu(S) \leqslant 1$ and $[0,1]$ are replaced by $\mu(S) \leqslant r$ and $[0, r]$ (respectively), and B is the σ-algebra generated by intervals in $[0, r]$. We stick to the case $r = 1$ to simplify the presentation. Probabilistic propositional modal logic (PPML) is generated by the grammar

$$\phi ::= \bot \mid q \mid \neg\phi \mid \phi \wedge \phi \mid [\mathrm{X}\phi]_{\sqsupseteq p}, \tag{1}$$

where $q \in \mathsf{AP}$, $p \in [0,1]$, and $\sqsupseteq \in \{\geqslant, >\}$. We often use that $r \geqslant s \sqsupseteq p$ implies $r \sqsupseteq p$ for all $\sqsupseteq \in \{\geqslant, >\}$. The last clause in (1) generates a probabilistic analogue of the temporal modality ne**X**t. The semantics of PPML assumes that, for all $\phi \in$ PPML, the set of states satisfying ϕ is measurable, i.e. in Σ.

Definition 2. Let $[\![\phi]\!]_M$ be the set of all $s \in S$ with $(M, s) \models \phi$, where

$$[\![\bot]\!] = \{\}, \qquad [\![q]\!] = L(q),$$
$$[\![\neg\phi]\!] = S \setminus [\![\phi]\!], \qquad [\![\phi_1 \wedge \phi_2]\!] = [\![\phi_1]\!] \cap [\![\phi_2]\!],$$
$$[\![[\mathrm{X}\phi]_{\sqsupseteq p}]\!] = \{s \in S \mid R(s, [\![\phi]\!]) \sqsupseteq p\}.$$

As in the definition above, we write $[\![\phi]\!]$ whenever M is determined by context. In particular, $(M, s) \models [\mathrm{X}\phi]_{\sqsupseteq p}$ holds if the probability of "a transition with source s having a target in which ϕ holds" is $\sqsupseteq p$, where "transition" refers to a state change $s \to s'$ governed by $R(s, \cdot)$. We write $\phi \vee \psi$ as a shorthand for $\neg(\neg\phi \wedge \neg\psi)$, and $\phi \to \psi$ as a shorthand for $\neg(\phi \wedge \neg\psi)$.

Example 3. Using negation one can derive operators $[\mathrm{X}\phi]_{<p}$ and $[\mathrm{X}\phi]_{\leqslant p}$ in PPML for stochastic kernels R for which all $\lambda A.R(s, A)$ have mass 1: the formula $[\mathrm{X}\neg\phi]_{>1-p}$ then

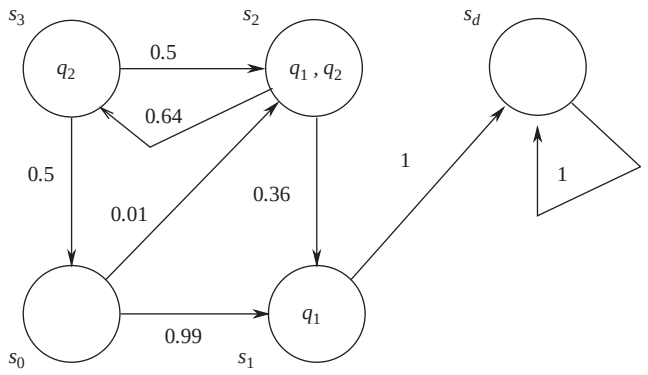

Fig. 1. A discrete labelled Markov chain with $\mathsf{AP} = \{q_1, q_2\}$. State s_d models deadlock.

states "the probability that ϕ is false in the next state is strictly greater than $1 - p$," i.e. "the probability that ϕ is true at the next state is strictly less than p." Therefore

$$[\mathrm{X}\phi]_{<p} \equiv [\mathrm{X}\neg\phi]_{>1-p}$$

and, similarly,

$$[\mathrm{X}\phi]_{\leqslant p} \equiv [\mathrm{X}\neg\phi]_{\geqslant 1-p}\,.$$

Proposition 4. *For all ϕ of PPML, $[\![\ \phi\ ]\!]$ is well defined and in Σ.*

Proof. We use structural induction on ϕ. By definition, $[\![\ \bot\ ]\!] = \{\} = S \setminus S \in \Sigma$. For atomic propositions, $[\![\ q\ ]\!] = L(q) \in \Sigma$ by the type of L. For $\neg\phi$ and $\phi_1 \wedge \phi_2$ this follows by induction since σ-algebras are closed under set complements and finite intersections. For $[\mathrm{X}\phi]_{\sqsupseteq p}$ this follows by induction since $\lambda s.R(s, [\![\ \phi\ ]\!])\colon (S, \Sigma) \to ([0,1], \mathsf{B})$ is measurable as R is a stochastic kernel, the sets $\{r \in [0,1] \mid r \sqsupseteq p\}$ with $\sqsupseteq \in \{\geqslant, >\}$ are in B, and therefore $[\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!] = (\lambda s.R(s, [\![\ \phi\ ]\!]))^{-1}(\{r \in [0,1] \mid r \sqsupseteq p\}) \in \Sigma$. □

Example 5. Let M be the labelled Markov chain with $\mathsf{AP} = \{q_1, q_2\}$ depicted in Fig. 1 where states are labelled with those propositions that hold at them and transitions are labelled with their probabilities. For example, $s_3 \in L(q_2)$, $s_0 \notin L(q_1)$, $R(s_0, \{s_2\}) = 0.01$, and $R(s_0, \{s_0, s_1, s_2\}) = 0 + 0.99 + 0.01 = 1$. We compute $[\![\ [\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}\ ]\!]$. Since $[\![\ q_1 \vee q_2\ ]\!] = \{s_1, s_2, s_3\}$ we have $[\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!] = \{s \in S \mid R(s, \{s_1, s_2, s_3\}) > 0\} = \{s_0, s_2, s_3\}$ and so $[\![\ \neg[\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!] = S \setminus \{s_0, s_2, s_3\} = \{s_1, s_d\}$. So $[\![\ [\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}\ ]\!] = \{s \in S \mid R(s, \{s_1, s_d\}) \geqslant 0.95\} = \{s_0, s_1, s_d\}$.

The labelled Markov chain in Fig. 1 has finitely many states. We now present a simple example of a labelled Markov chain with an uncountable set of states.

Example 6. Let $S = [0, 1]$, $\mathsf{AP} = \{q\}$, $L(q) = \{0, 1\}$, and $\Sigma = \mathsf{B}$. For each $s \in [0, 1]$ and $A \in \mathsf{B}$ let $R(s, A)$ be

- 0 if neither $s/2$ nor $s + (1 - s)/2$ are in A,
- if both are in A,
- s if only $s/2$ is in A, and
- $1 - s$ if only $s + (1 - s)/2$ is in A.

As the predicates in this definition are based on measurable functions, this defines a stochastic kernel. We compute $[\![\neg[\mathrm{X}q]_{>0}]\!] = S \setminus \{s \in [0, 1] \mid s/2 = 0 \text{ or } s + (1 - s)/2 = 1\} = S \setminus \{0, 1\} = (0, 1)$.

4. Three-valued approximants for PPML

Three-valued abstraction-based model checking (see e.g. [5,6,9,10,21,31]) is a technique for verifying properties of models by verifying them on abstract, notably finite-state, models. In using three-valued models and checks, one gains that the verification and refutation of properties conducted on abstract models apply to the concrete one as well, even if properties nest path quantifiers and negations. We now develop such an abstraction technique for labelled Markov chains and PPML and extend it to full PCTL in Section 6.

The three-valued approach to labelled Markov chains presented below shares with the two-valued work by Danos and Desharnais [12] that abstract models are generally not probabilistic (in particular, no longer labelled Markov chains), *but quantitative* systems in that the set-valued functions that serve as abstractions of measures lose the additivity property but retain continuity properties. These continuity properties reduce to monotonicity in this paper as we work with finite-state abstractions only. These abstract models are called pre-LMPs in the event-based setting of loc. cit. Abstraction often extends the notion of model, e.g. in moving from deterministic programs to non-deterministic models through the abstraction of control flow. As demonstrated in loc. cit., this broadening of the notion of model and its property semantics allows for the construction of more precise, even optimal finite-state abstractions. We extend those optimality results to PPML by combining finite-state and state-based versions of pre-LMPs and sup-pre-LMPs in loc. cit. The unrestricted negation of PPML requires mild and always realizable conditions on state-space partitions used for proving such optimality. A state-space partition determines an abstraction relation $s \rho t$ by relating a concrete state s with the unique partition t in which it resides.

Definition 7. For the remainder of this paper let $\hat{S}$ be a designated *finite* set of abstract states with a relation $\rho \subseteq S \times \hat{S}$ that is left-total ($\forall s \in S\, \exists t \in \hat{S}\colon s \rho t$) and right-total ($\forall t \in \hat{S}\, \exists s \in S\colon s \rho t$) for a labelled Markov chain $M = (S, \Sigma, R, L)$. For $A \subseteq S$ and $B \subseteq \hat{S}$ let

$$A.\rho = \{t \in \hat{S} \mid \exists s \in A\colon s \rho t\},$$
$$\rho.B = \{s \in S \mid \exists t \in B\colon s \rho t\}.$$

Any such relation ρ is merely an alternative way of representing certain abstract interpretations [8]. We refer to [34] for an account of how to move between such different ways of representing abstract interpretations.

Example 8. Let F be a finite set of formula of PPML and let A be the subset of those $q \in \mathsf{AP}$ that appear in some formula in F. Define an equivalence relation $Q_A \subseteq S \times S$ by $(s, s') \in Q_A$ iff (for all $q \in A$, $s \models q$ iff $s' \models q$). Let $\hat{S}$ be the set of equivalence classes of Q_A and let $s \rho t$ mean $s \in t$. Then $\hat{S}$ is finite, and ρ is left-total and right-total. Moreover, $\rho.\{t\} = \rho.\{t'\}$ implies $t = t'$.

Using $\rho \subseteq S \times \hat{S}$ we define an abstract version $\hat{M}$ of the labelled Markov chain $M = (S, \Sigma, R, L)$ with state set $\hat{S}$ and measure space $(\hat{S}, \mathbb{P}(\hat{S}))$, specify a three-valued semantics for PPML on $\hat{M}$, and show that properties verified on $\hat{M}$ are also true in M. Each abstract version of R and L occurs in two modes $m \in \{a, c\}$, where a stands for "asserted" and c for "consistent" [26] and constitutes the aforementioned must- and may-structure (respectively). The mode a under-approximates whereas mode c over-approximates structure in M. The definition of the labelling functions $\hat{L}^m \colon \mathsf{AP} \to \mathbb{P}(\hat{S})$ are standard (see e.g. [9,10]):

$$\hat{L}^a(q) = \{t \in \hat{S} \mid \rho.\{t\} \subseteq L(q)\}, \quad \hat{L}^c(q) = L(q).\rho \tag{2}$$

for all $q \in \mathsf{AP}$. The functions

$$\hat{R}^m \colon \hat{S} \times \mathbb{P}(\hat{S}) \to [0, 1]$$

utilize inner and outer measures and are defined by

$$\hat{R}^a(t, B) = inf\{R(s, \rho.B)^* \mid s \rho t\} \quad \hat{R}^c(t, B) = sup\{R(s, \rho.B)_* \mid s \rho t\} \tag{3}$$

for all $t \in \hat{S}$ and $B \subseteq \hat{S}$. Intuitively, $\hat{R}^a(t, B)$ and $\hat{R}^c(t, B)$ are abstractions of the probability that a transition from any state s with $s \rho t$ enters the set $\rho.B$. Since measures μ are monotone, we have $\mu_* \leqslant \mu^*$ and so $\hat{R}^a(t, B) \leqslant \hat{R}^c(t, B)$ for all $t \in \hat{S}$ and $B \subseteq \hat{S}$. For each $t \in \hat{S}$ and $m \in \{a, c\}$ the functions

$$\lambda B.\hat{R}^m(t, B) \colon \hat{S} \to [0, 1]$$

are monotone and map $\{\}$ to 0; yet, as already noted in [12], they are not additive, i.e. finite measures, in general.

The most dramatic consequence of losing non-additivity concerns the representation of set-valued monotone maps. Unlike measures, such maps can no longer be encoded through a vector of values for singleton sets. This poses a significant challenge for implementing these techniques in probabilistic model checkers and addressing this challenge is beyond the scope of this paper. That abstractions of measures are not additive in general is illustrated in the next example.

Example 9. Let M be as in Example 5 and Fig. 1. Let $\hat{S} = \{t_0, t_1, t_d\}$, $\rho.\{t_0\} = \{s_0, s_1\}$, $\rho.\{t_1\} = \{s_2, s_3\}$, and $\rho.\{t_d\} = \{s_d\}$. Fig. 2 depicts the resulting abstract model. For any $q \in \mathsf{AP}$ a tag $q?$ at state t indicates $t \in \hat{L}^c(q) \setminus \hat{L}^a(q)$, whereas q at t denotes $t \in \hat{L}^a(q)$. If neither q nor $q?$ appear at t, then $t \notin \hat{L}^c(q)$. Transitions from t to t' are labelled with the interval $[\hat{R}^a(t, \{t'\}), \hat{R}^c(t, \{t'\})]$. Note that the measure $\lambda B.\sum_{t' \in B} \hat{R}^c(t_1, \{t'\})$ has mass 1.14 and so $\lambda B.\hat{R}^c(t_1, B)$ is not additive as its mass is $\leqslant 1$.

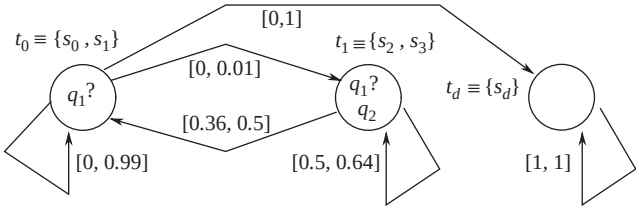

Fig. 2. Abstract probabilities $\hat{R}^m(t, \{t'\})$ and labels $\hat{L}^m(q)$ for Example 9. Transitions from t to t' are labelled with $[\hat{R}^a(t, \{t'\}), \hat{R}^c(t, \{t'\})]$. For any $q \in \mathsf{AP}$ labels q, $q?$, and their absence at t mean $t \in \hat{L}^a(q)$, $t \in \hat{L}^c(q) \setminus \hat{L}^a(q)$, and $t \notin \hat{L}^c(q)$ (respectively). This figure does not depict the complete abstract model as only abstract transitions to singleton sets, not to arbitrary sets, are shown.

We now re-visit Example 6 and specify an abstraction of its concrete model induced by a state partition. This partition is determined by a finite set of PPML formulas and already illustrates the principles used for the optimality results developed in this paper.

Example 10. Let M be as in Example 6. For $\mathsf{F} = \{\neg[\mathrm{X}q]_{>0}\}$ let $\langle\mathsf{F}\rangle = \{q, [\mathrm{X}q]_{>0}, \neg[\mathrm{X}q]_{>0}\}$ be the set of sub-formulas of F. We partition S such that equivalence classes satisfy exactly the same formulas in $\langle\mathsf{F}\rangle$. Since $(M, s) \models q \to [\mathrm{X}q]_{>0}$ holds for all $s \in S$, we get $\hat{S} = \{t_0, t_1\}$ with $\rho.\{t_0\} = \{0, 1\}$ and $\rho.\{t_1\} = (0, 1)$. We have $\hat{L}^c(q) = \hat{L}^a(q) = \{t_0\}$. Furthermore, we have $[\hat{R}^a(t_0, \{t_0\}), \hat{R}^c(t_0, \{t_0\})] = [1, 1]$ and $[\hat{R}^a(t_1, \{t_1\}), \hat{R}^c(t_1, \{t_1\})] = [1, 1]$, and all other abstract values $\hat{R}^m(t_i, \{t_j\})$ are 0 whenever $i \neq j$.

The abstract semantics of PPML on $\hat{M}$ is stated via two satisfaction predicates $\models m$ with $m \in \{a, c\}$. The connection to three-valued model checking, as presented in [5], is that at state t property ϕ has

- value 1 (definitely holds, a *verification*) if $(\hat{M}, t) \models a\phi$,
- value 0 (definitely does not hold, a *refutation*) if $(\hat{M}, t) \not\models c\phi$, and
- value $1/2$ (may or may not hold, an *inconclusive check*) otherwise.

So a check of ϕ at t is inconclusive iff $((\hat{M}, t) \not\models a\phi$ and $(\hat{M}, t) \models c\phi)$.

Definition 11. Let $[\![\ \phi\ ]\!]^m_{\hat{M}} = \{t \in \hat{S} \mid (\hat{M}, t) \models m\phi\}$, $\neg a = c$, $\neg c = a$, and

$$
\begin{array}{ll}
[\![\ \bot\ ]\!]^m = \{\}, & [\![\ q\ ]\!]^m = \hat{L}^m(q), \\
[\![\ \neg\phi\ ]\!]^m = \Sigma \setminus [\![\ \phi\ ]\!]^{\neg m}, & [\![\ \phi_1 \wedge \phi_2\ ]\!]^m = [\![\ \phi_1\ ]\!]^m \cap [\![\ \phi_2\ ]\!]^m, \\
[\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^m = \{t \in \hat{S} \mid \hat{R}^m(t, [\![\ \phi\ ]\!]^m) \sqsupseteq p\}, & (m \in \{a, c\})\,.
\end{array}
$$

As before, we elide $\hat{M}$ in $[\![\ \phi\ ]\!]^m$ and do so whenever $\hat{M}$ is determined by context. We show that the interpretation $[\![\ \phi\ ]\!]^m$ is sound in that verifications in $\hat{M}$ are verifications in M and refutations in $\hat{M}$ are refutations in M, mediated by ρ. In doing so no assumptions are made about the measurability of sets of the form $\rho.B$, although such assumptions are guaranteed by construction, and used, for optimal approximants subsequently.

Theorem 12. *For all ϕ of PPML we have $\rho.[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]$, $[\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^c$, and $[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]^c$.*

Proof. We show the first two claims by structural induction on ϕ, using Proposition 4 repeatedly. The inductive arguments for all operators except X are standard (see e.g. [5] or [26]) and omitted.

(1) Let $t \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^a$ and $s\rho t$. We need to show $s \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]$. From $t \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^a$ we infer $inf\{R(\bar{s}, \rho.[\![\ \phi\ ]\!]^a)^* \mid \bar{s}\rho t\} \sqsupseteq p$ by (3). Since $s\rho t$ we therefore have $R(s, \rho.[\![\ \phi\ ]\!]^a)^* \geqslant inf\{R(\bar{s}, \rho.[\![\ \phi\ ]\!]^a)^* \mid \bar{s}\rho t\} \sqsupseteq p$ and so $R(s, \rho.[\![\ \phi\ ]\!]^a)^* \sqsupseteq p$. By induction, $\rho.[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]$. But $[\![\ \phi\ ]\!] \in \Sigma$ by Proposition 4. Therefore, $R(s, [\![\ \phi\ ]\!]) \geqslant R(s, \rho.[\![\ \phi\ ]\!]^a)^* \sqsupseteq p$. Thus, $s \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]$.

(2) Let $s \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]$ and $s\rho t$. We need to show $t \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^c$. From $s \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]$ we infer $R(s, [\![\ \phi\ ]\!]) \sqsupseteq p$. By induction, $[\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^c$ which implies $[\![\ \phi\ ]\!] \subseteq \rho.([\![\ \phi\ ]\!].\rho) \subseteq \rho.[\![\ \phi\ ]\!]^c$ as ρ is left-total and $B \mapsto \rho.B$ is monotone (respectively). By Proposition 4, $[\![\ \phi\ ]\!] \in \Sigma$ and so $[\![\ \phi\ ]\!] \subseteq \rho.[\![\ \phi\ ]\!]^c$ implies $R(s, \rho.[\![\ \phi\ ]\!]^c)_* = sup\{R(s, X) \mid \rho.[\![\ \phi\ ]\!]^c \supseteq X \in \Sigma\} \geqslant R(s, [\![\ \phi\ ]\!]) \sqsupseteq p$. Thus $R(s, \rho.[\![\ \phi\ ]\!]^c)_* \sqsupseteq p$. Since $s\rho t$ the latter renders $\hat{R}^c(t, [\![\ \phi\ ]\!]^c) = sup\{R(\bar{s}, \rho.[\![\ \phi\ ]\!]^c)_* \mid \bar{s}\rho t\} \geqslant R(s, \rho.[\![\ \phi\ ]\!]^c)_* \sqsupseteq p$. Thus, $\hat{R}^c(t, [\![\ \phi\ ]\!]^c) \sqsupseteq p$ which means $t \in [\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^c$.

Finally, $[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]^c$ is a consequence of the first two claims: we have $[\![\ \phi\ ]\!]^a \subseteq (\rho.[\![\ \phi\ ]\!]^a).\rho$ since ρ is right-total and therefore $[\![\ \phi\ ]\!]^a \subseteq (\rho.[\![\ \phi\ ]\!]^a).\rho \subseteq [\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^c$ as $A \mapsto A.\rho$ is monotone. □

Example 13. We compute $[\![\ \phi\ ]\!]^m$ for ϕ being $[\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}$, $m \in \{a, c\}$, and the model in Example 9. First, $[\![\ q_1 \vee q_2\ ]\!]^c = \{t_0, t_1\} \cup \{t_1\} = \{t_0, t_1\}$ and so $[\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^c = \{t \in \hat{S} \mid \hat{R}^c(t, \{t_0, t_1\}) > 0\} = \{t_0, t_1\}$. Thus, $[\![\ \neg[\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^a = \hat{S} \setminus [\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^c = \{t_d\}$ and therefore $[\![\ \phi\ ]\!]^a = \{t \in \hat{S} \mid \hat{R}^a(t, \{t_d\}) \geqslant 0.95\} = \{t_d\}$. Dually, $[\![\ q_1 \vee q_2\ ]\!]^a = \{t_1\}$ and so $[\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^a = \{t \in \hat{S} \mid \hat{R}^a(t, \{t_1\}) > 0\} = \{t_1\}$. Therefore, we get $[\![\ \neg[\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^c = \hat{S} \setminus [\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^a = \{t_0, t_d\}$ and so $[\![\ \phi\ ]\!]^c = \{t \in \hat{S} \mid \hat{R}^c(t, \{t_0, t_d\}) \geqslant 0.95\} = \{t_0, t_d\}$. So the check of ϕ is inconclusive at t_0 but conclusive at t_1 (a refutation) and t_d (a verification). By soundness, ϕ is false at s_2 and s_3.

From Definition 11 it is easily seen that Theorem 12 remains valid if we further under-approximate all must-structure and over-approximate all may-structure in $\hat{M}$, where these further approximations are denoted with a tilde: $\tilde{R}^a(t, B) \leqslant \hat{R}^a(t, B)$, $\tilde{L}^a(q) \subseteq \hat{L}^a(q)$; and $\hat{R}^c(t, B) \leqslant \tilde{R}^c(t, B)$, $\hat{L}^c(q) \subseteq \tilde{L}^c(q)$ for all $t \in \hat{S}$, $B \subseteq \hat{S}$, and $q \in \mathsf{AP}$. This property is vital for the practical applicability of the approach proposed here, as the structure defined on $\hat{M}$ may not be computable or only computable in the limit.

Since the functions $\lambda B.\hat{R}^m(t, B)$ are generally not additive (recall Example 9), we may have to pay an exponential penalty in representing $\hat{M}$, as all values $\hat{R}^m(t, B)$ with $B \subseteq \hat{S}$ may have to be generated. In case this is undesired, one can approximate each $\lambda B.\hat{R}^m(t, B)$ by the finite measure $\lambda B.\tilde{R}^m(t, B)\colon \mathbb{P}(\hat{S}) \to [0, r_m]$ defined by

$$\lambda B.\tilde{R}^m(t, B) = \lambda B.\sum_{t' \in B} \hat{R}^m(t, \{t'\}),$$

where r_a may be chosen as 1 and r_c as the size of $\hat{S}$. These bounds on total masses are sound since $\lambda B.\tilde{R}^a(t,B) \leqslant \lambda B.\hat{R}^a(t,B)$ and $\lambda B.\hat{R}^c(t,B) \leqslant \lambda B.\tilde{R}^c(t,B)$ for all $t \in \hat{S}$. (Summation over an empty index set is defined to be 0.) We retain the abstraction of labels in (2) in defining the modified semantics $[\![\ \phi\ ]\!]^{\tilde{m}}$. All clauses for $[\![\ \phi\ ]\!]^{\tilde{m}}$ are compositional in $[\![\ \phi\ ]\!]^{\tilde{m}}$ and mimic the ones for $[\![\ \phi\ ]\!]^m$ except for

$$[\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^{\tilde{m}} = \{t \in \hat{S} \mid \tilde{R}^m(t, [\![\ \phi\ ]\!]^{\tilde{m}}) \sqsupseteq p\}\,.$$

So $[\![\ \phi\ ]\!]^{\tilde{m}}$ checks PPML formulas in a style familiar from finite-state Markov chains.

Remark 14. For all ϕ of PPML and $m \in \{a, c\}$ we have

$$[\![\ \phi\ ]\!]^{\tilde{a}} \subseteq [\![\ \phi\ ]\!]^a \quad \text{and} \quad [\![\ \phi\ ]\!]^c \subseteq [\![\ \phi\ ]\!]^{\tilde{c}},$$

and Theorem 12 applies with the modified semantics $[\![\ \phi\ ]\!]^{\tilde{m}}$ instead of $[\![\ \phi\ ]\!]^m$.

Example 15. Consider the model $\hat{M}$ in Fig. 2.

(1) Computing $[\![\ [\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}\ ]\!]^{\tilde{a}}$ and $[\![\ [\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}\ ]\!]^{\tilde{c}}$ proceeds as in Example 13 for a and c (respectively), and yields the same results, but the evaluation of formulas of the form $[\mathrm{X}\phi]_{\sqsupseteq p}$ is different: $[\![\ [\mathrm{X}(q_1 \vee q_2)]_{>0}\ ]\!]^{\tilde{c}} = \{t \in \hat{S} \mid \hat{R}^c(t,\{t_0\}) + \hat{R}^c(t,\{t_1\}) > 0\}$ and therefore $[\![\ [\mathrm{X}\neg[\mathrm{X}(q_1 \vee q_2)]_{>0}]_{\geqslant 0.95}\ ]\!]^{\tilde{c}} = \{t \in \hat{S} \mid \hat{R}^c(t,\{t_0\}) + \hat{R}^c(t,\{t_d\}) \geqslant 0.95\}$. This coincidence of meaning is not always the case, as demonstrated in the next item.

(2) For ϕ being $[\mathrm{X}\neg q_2]_{>0}$, we have $t_0 \notin [\![\ \phi\ ]\!]^{\tilde{a}}$ as $[\![\ \neg q_2\ ]\!]^{\tilde{a}} = \{t_0, t_d\}$ and $\hat{R}^a(t_0,\{t_0\}) + \hat{R}^a(t_0,\{t_d\}) = 0 + 0 = 0$. But $t_0 \in [\![\ \phi\ ]\!]^a$ as $[\![\ \neg q_2\ ]\!]^a = \{t_0, t_d\}$ and $\hat{R}^a(t_0,\{t_0,t_d\}) = \mathit{inf}\{R(s_0,\{s_0,s_1,s_d\}), R(s_1,\{s_0,s_1,s_d\})\} = \mathit{inf}\{0.99, 1\} > 0$. Thus, $t_0 \in [\![\ \phi\ ]\!]^a \setminus [\![\ \phi\ ]\!]^{\tilde{a}}$ and the additive semantics is inconclusive for t_0 whereas the non-additive one is conclusive.

We re-visit Example 10 and see that its model is an optimal abstraction for the considered finite set of PPML formulas.

Example 16. Consider the abstraction in Example 10. Since $\hat{L}^c(q) = \{t_0\}$ we get $[\![\ [\mathrm{X}q]_{>0}\ ]\!]^{\tilde{c}} = \{t \in \hat{S} \mid \hat{R}^c(t,\{t_0\}) > 0\} = \{t_0\}$ and so $[\![\ \neg[\mathrm{X}q]_{>0}\ ]\!]^{\tilde{a}} = \{t_1\}$. Since $\rho.\{t_1\} = (0,1)$, this finite approximant and $[\![\ \neg[\mathrm{X}q]_{>0}\ ]\!]^{\tilde{a}}$ are "optimal" for the property $\neg[\mathrm{X}q]_{>0}$.

We generalize an optimality result by Danos and Desharnais [12].

Definition 17. For a finite set F of formulas of PPML, $(\hat{M}, \rho)$ is *optimal for* F *and* M iff

$$\forall \phi \in \mathsf{F}\ \forall s \rho t\colon s \in [\![\ \phi\ ]\!] \text{ iff } t \in [\![\ \phi\ ]\!]^a\,. \tag{4}$$

In particular, we then have $[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!]^c$ for all such formulas, meaning that model checks in $\hat{M}$ are guaranteed to be conclusive for all checks drawn from F. Since PPML has unrestricted negation, conditions on ρ are required but can always be enforced for guaranteeing such optimality in Theorem 21 below.

Definition 18. For a finite set F of PPML formulas, let

$$\langle \mathsf{F} \rangle = \mathsf{F} \cup \{\psi |\ \psi \text{ sub-formula of a formula in } \mathsf{F}\}\,.$$

Define an equivalence relation $Q_{\mathsf{F}} \subseteq S \times S$ by

$$(s_1, s_2) \in Q_{\mathsf{F}} \text{ iff for all } \phi \in \langle \mathsf{F} \rangle,\ (s_1 \in [\![\ \phi\ ]\!] \text{ iff } s_2 \in [\![\ \phi\ ]\!])\,.$$

Clearly, $\langle \mathsf{F} \rangle$ is finite whenever F is. As noted in [12], since Σ is closed under set complements and finite intersections, each equivalence class of Q_{F} is in Σ and is closed under meanings from $\langle \mathsf{F} \rangle$:

$$\forall \phi \in \langle \mathsf{F} \rangle : [\![\ \phi\ ]\!].Q_{\mathsf{F}} \subseteq [\![\ \phi\ ]\!]\,.$$

Definition 19. Let Q be any equivalence relation with $Q \subseteq Q_{\mathsf{F}}$. Let $\hat{S}$ be the set of equivalence classes of S with respect to Q and define $s \rho t$ to mean $s \in t$.

The ρ of Definition 19 is left-total, right-total, and $\rho.\{t\} \cap \rho.\{t'\} \neq \{\}$ implies $t = t'$. We claim that any such model is optimal for all formulas of F under some restrictions on Q. For that, it is useful to recognize several equivalent ways of expressing optimality (4) of an abstraction.

Lemma 20. *If $\rho.\{t\} \cap \rho.\{t'\} \neq \{\}$ implies $t = t'$ for all $t, t' \in \hat{S}$, the following are equivalent for all $\phi \in PPML$:*
(1) $[\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^a$ *and* $\rho.[\![\ \phi\ ]\!]^c \subseteq [\![\ \phi\ ]\!]$
(2) $[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!]^c$
(3) $[\![\ \phi\ ]\!] = \rho.[\![\ \phi\ ]\!]^c = \rho.[\![\ \phi\ ]\!]^a$.

Proof.
- (1) implies (2): $[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]^c$ by Theorem 12. Also, $[\![\ \phi\ ]\!]^c \subseteq (\rho.[\![\ \phi\ ]\!]^c).\rho \subseteq [\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^a$ where the last two inclusions follow from item (1) and the monotonicity of $A \mapsto A.\rho$, and the first one from the right-totality of ρ.
- (2) implies (3): $\rho.[\![\ \phi\ ]\!]^c = \rho.[\![\ \phi\ ]\!]^a$ by item (2) and $\rho.[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]$ by Theorem 12. To show $[\![\ \phi\ ]\!] \subseteq \rho.[\![\ \phi\ ]\!]^a$ let $s \in [\![\ \phi\ ]\!]$. Then there is some $t \in \hat{S}$ with $s \rho t$ as ρ is left-total, so $t \in [\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^c$ by Theorem 12. By item (2), $t \in [\![\ \phi\ ]\!]^c = [\![\ \phi\ ]\!]^a$ and so $s \in \rho.[\![\ \phi\ ]\!]^a$.
- (3) implies (1): By item (3), $[\![\ \phi\ ]\!].\rho = (\rho.[\![\ \phi\ ]\!]^a).\rho$ but the latter is in $[\![\ \phi\ ]\!]^a$ by the assumption on ρ. By item (3) we also have $\rho.[\![\ \phi\ ]\!]^c \subseteq [\![\ \phi\ ]\!]$. □

In [15] probabilistic bisimulation is characterized by a simple temporal logic without negation. Negation adds expressiveness to such a logic. For any $q \in \mathsf{AP}$ a "nil" state is characterized by $\neg[\mathrm{X}(q \vee \neg q)]_{>0}$: a state s satisfies this formula iff $R(s, S) = 0$, i.e. $\lambda A.R(s, A) = \lambda A.0$ by monotonicity. The expressiveness of negation adds a complication to securing the optimality result in (4). Technically one needs that the abstraction relation ρ meshes well with the concrete meanings of all formulas of the form $[\mathrm{X}\phi]_{\sqsupseteq p}$ in $\langle \mathsf{F} \rangle$. Formally, conditions (5) and (6) below are required. These conditions are much weaker than state-based notions of probabilistic simulation equivalence but hold for such equivalences.

Before we state and prove this optimality theorem, we discuss its two conditions

$$[\mathrm{X}\phi]_{\geqslant p} \in \langle \mathsf{F} \rangle,\ \mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} < p \Rightarrow \mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \neq p, \tag{5}$$

$$[\mathrm{X}\phi]_{>p} \in \langle \mathsf{F} \rangle,\ \mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} > p \Rightarrow \mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \neq p. \tag{6}$$

Condition (5) states that for all formulas of the form $[\mathrm{X}\phi]_{\geqslant p}$ for which one wants optimality one needs: "If $R(\bar{s}, [\![\ \phi\ ]\!])$ is strictly less than p for some concrete state $\bar{s}$ related to the abstract state t (which is equivalent to the inequality $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} < p$), then the upper bound of all such values $R(\bar{s}, [\![\ \phi\ ]\!])$ ranging over such concrete $\bar{s}$ cannot be p (and is then strictly less than p)." Put informally, if the abstract transition value $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\}$ is strictly below the value p for a threshold $\geqslant p$ in a formula for which one wants to gain optimality, then $\mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\}$ also needs to be strictly below p. Condition (6) is similar but concerns all thresholds $> p$ and has the roles of *inf* and *sup* swapped.

Theorem 21. *Let* F *be a finite subset of PPML and* $\hat{M}$ *as in Definition* 19. *Then* (4) *holds whenever for all* $t \in \hat{S}$ *we have* (5) *and* (6).

Proof. By Lemma 20 it suffices to show $[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!]^c$ for all $\phi \in \langle \mathsf{F} \rangle$ by simultaneous structural induction on ϕ. Since $[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]^c$ by Theorem 12, it suffices to show $[\![\ \phi\ ]\!]^c \subseteq [\![\ \phi\ ]\!]^a$ but we may still assume equality, and even $[\![\ \phi\ ]\!] = \rho.[\![\ \phi\ ]\!]^c = \rho.[\![\ \phi\ ]\!]^a$ inductively, by Lemma 20.

- For $\bot$ there is nothing to show and the cases for negation and conjunction simply appeal to their semantics and induction.
- Let $q \in \langle \mathsf{F} \rangle$ and $t \in \hat{S}$. Since $Q \subseteq Q_{\mathsf{F}}$, either $\rho.\{t\}$ is contained in $L(q)$ or $\rho.\{t\}$ has empty intersection with $L(q)$ and so $[\![\ q\ ]\!]^a = [\![\ q\ ]\!]^c$.
- Let $[\mathrm{X}\phi]_{\geqslant p} \in \langle \mathsf{F} \rangle$. Then $\phi \in \langle \mathsf{F} \rangle$. By induction, $[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!]^c$ and so, by Lemma 20, $[\![\ \phi\ ]\!] = \rho.[\![\ \phi\ ]\!]^c = \rho.[\![\ \phi\ ]\!]^a$ which is in Σ by Proposition 4. Let $t \in [\![\ [\mathrm{X}\phi]_{\geqslant p}\ ]\!]^c$ and so, as $\rho.[\![\ \phi\ ]\!]^c = [\![\ \phi\ ]\!] \in \Sigma$,

$$\mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \geqslant p\,. \tag{7}$$

  To show $t \in [\![\ [\mathrm{X}\phi]_{\geqslant p}\ ]\!]^a$ it therefore suffices to show $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \geqslant p$ as $\rho.[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!] \in \Sigma$. Proof by contradiction: Let $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \not\geqslant p$, i.e. $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} < p$. Then there is some $\tilde{s}$ with $\tilde{s}\rho t$ and $R(\tilde{s}, [\![\ \phi\ ]\!]) < p$ and so $\tilde{s} \notin [\![\ [\mathrm{X}\phi]_{\geqslant p}\ ]\!]$, i.e. $\bar{s} \notin [\![\ [\mathrm{X}\phi]_{\geqslant p}\ ]\!]$ for all $\bar{s}\rho t$ as $Q \subseteq Q_{\mathsf{F}}$. Therefore, $\mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \leqslant p$ which, together with (7), contradicts (5) since $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} < p$.
- Let $[\mathrm{X}\phi]_{>p} \in \langle \mathsf{F} \rangle$. Then $\phi \in \langle \mathsf{F} \rangle$. By induction, $[\![\ \phi\ ]\!]^a = [\![\ \phi\ ]\!]^c$ and so, by Lemma 20 and Proposition 4, $[\![\ \phi\ ]\!] = \rho.[\![\ \phi\ ]\!]^c = \rho.[\![\ \phi\ ]\!]^a \in \Sigma$. Let $t \in [\![\ [\mathrm{X}\phi]_{>p}\ ]\!]^c$ and so

$$\mathit{sup}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} > p\,. \tag{8}$$

  To show $t \in [\![\ [\mathrm{X}\phi]_{>p}\ ]\!]^a$ it therefore suffices to show $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} > p$. From (8) we infer the existence of some $\tilde{s}$ with $\tilde{s}\rho t$ and $R(\tilde{s}, [\![\ \phi\ ]\!]) > p$ and so $\tilde{s} \in [\![\ [\mathrm{X}\phi]_{>p}\ ]\!]$. Thus, $R(\bar{s}, [\![\ \phi\ ]\!]) > p$ for all $\bar{s}$ with $\bar{s}\rho t$ as $Q \subseteq Q_{\mathsf{F}}$, implying $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} \geqslant p$. The latter, in conjunction with (6) and (8), renders $\mathit{inf}\{R(\bar{s}, [\![\ \phi\ ]\!]) \mid \bar{s}\rho t\} > p$ and so $t \in [\![\ [\mathrm{X}\phi]_{>p}\ ]\!]^a$. □

Conditions (5) and (6), if false, are enforced by making conditional changes to thresholds in ϕ in a bottom-up fashion: whenever (5) (respectively (6)) is false, change $[\mathrm{X}\phi]_{\geqslant p}$ to $[\mathrm{X}\phi]_{\geqslant p-\varepsilon}$ (respectively $[\mathrm{X}\phi]_{>p}$ to $[\mathrm{X}\phi]_{>p+\varepsilon}$) for any $\varepsilon > 0$.

Example 22. In Example 16 we already encountered an optimal model check; it is an instance of Theorem 21: Since $[\![[\mathrm{X}q]_{>0}]\!] = \{0, 1\}$ and $\sqsupseteq p$ is > 0, the implication in (5) holds as its premise is false. As for the implication in (6), its premise is false for $t = t_1$ but for $t = t_0$ it computes to $sup\{1, 1\} > 0$ and so its conclusion holds as $inf\{1, 1\} = 1$ is different from 0.

It would be of interest to determine whether similar optimality results can be secured for the additive semantics $[\![\phi]\!]^{\tilde{a}}$ and for formulas with the temporal operator "Until."

5. Probabilistic computation tree logic for labelled Markov chains

We extend the concrete and abstract semantics and their sound relationship from PPML to PCTL. The syntax of PCTL is generated by adding to (1) the clause $[\phi\,\mathrm{U}^{\leqslant k}\,\phi]_{\sqsupseteq p}$ where $k \in \mathbb{N} \cup \{\infty\}$:

$$\phi ::= \bot \mid q \mid \neg\phi \mid \phi \wedge \phi \mid [\mathrm{X}\phi]_{\sqsupseteq p} \mid [\phi\,\mathrm{U}^{\leqslant k}\,\phi]_{\sqsupseteq p}\,. \tag{9}$$

The intuitive meaning of $[\phi_1\,\mathrm{U}^{\leqslant k}\,\phi_2]_{\sqsupseteq p}$ is that the probability of all paths satisfying the path formula $\phi_1\mathrm{U}\phi_2$ within k steps is $\sqsupseteq p$. This fragment of PCTL is adequate and can express the temporal operator "weak Until" and all probabilistic interpretations of CTL connectives [22]. This may seem surprising as the grammar in (9) has the look-and-feel of a linear notion of time, whereas CTL is a branching-time temporal logic. But the path quantifiers for branching-time may be expressed as [22]

$$\mathrm{AX}\phi \equiv [\mathrm{X}\phi]_{\geqslant 1}, \quad \mathrm{EX}\phi \equiv [\mathrm{X}\phi]_{>0}$$

for the next-state temporal operator, and other temporal operators are quantified in the same manner.

For our semantics of PCTL on labelled Markov chains M, the meaning of all PPML operators is as already defined. The meaning of the temporal operator "Until" requires basic machinery from domain and measure theory to ensure that all sets $[\![\phi]\!]$ are in Σ. The definition below assumes Markowsky's result [32] that suprema of all countable directed subsets exist if suprema for all countable chains exist.

Definition 23. A *countable chain* in a partial order $(P, \leqslant)$ is a sequence $(x_n)_{n\in\mathbb{N}}$ in P such that $n \leqslant n'$ implies $x_n \leqslant x'_n$ for all $n, n' \in \mathbb{N}$. An *ω-dcpo* ("dcpo" stands for "*directed complete partial order*" [1]) is a partial order $(D, \leqslant)$ such that all countable chains of D have a supremum in D. An element $b \in D$ with $b \leqslant d$ for all $d \in D$ is called a *bottom element* of D (which is unique if it exists). A function $f\colon (D, \leqslant) \to (E, \leqslant)$ between ω-dcpos is *ω-continuous* iff f preserves the suprema of all countable chains $(x_n)_{n\in\mathbb{N}}$ of D: $f(sup\{x_n \mid n \in \mathbb{N}\}) = sup\{f(x_n) \mid n \in \mathbb{N}\}$.

Lemma 24. *Given an ω-continuous self map $f\colon (D, \leqslant) \to (D, \leqslant)$ on an ω-dcpo D with bottom element b, the least fixed point of f exists and is given by $sup_{n\in\mathbb{N}} f^n(b)$, where $f^0 = \lambda d.d$ and $f^{n+1} = f \circ f^n$ for all $n \in \mathbb{N}$.*

Proof. If $x \leqslant y$ in D, then $(z_n)_{n\in\mathbb{N}} = (x, y, y, \ldots)$ is a countable chain and so $f(y) = f(sup\{z_n \mid n \in \mathbb{N}\}) = sup\{f(z_n) \mid n \in \mathbb{N}\} = sup\{f(x), f(y)\}$ shows $f(x) \leqslant f(y)$. Thus, f is monotone. By monotonicity and ω-continuity of f, $(f^n(b))_{n\in\mathbb{N}}$ is a countable chain and $x = sup_{n\in\mathbb{N}} f^n(b)$ exists and is the least fixed point of f. □

A folklore result in measure theory captures that the set of measurable functions $f\colon (S, \Sigma) \to ([0, 1], \mathsf{B})$ forms an ω-dcpo. So we may use Lemma 24 to compute the meaning of the temporal operator "Until" as a measurable function.

Definition 25. (1) Let $\mathsf{M}(S, \Sigma)$ be the set of measurable functions $f\colon (S, \Sigma) \to ([0, 1], \mathsf{B})$, ordered point-wise: $f \leqslant g$ iff for all $s \in S$, $f(s) \leqslant g(s)$.

(2) For ϕ_1, ϕ_2 of PCTL, define a function $F(\phi_1, \phi_2)\colon \mathsf{M}(S, \Sigma) \to \mathsf{M}(S, \Sigma)$ by

$$F(\phi_1, \phi_2)(f) = \max\left(\chi_{[\![\phi_2]\!]}, \min\left(\chi_{[\![\phi_1]\!]}, \lambda s. \int f(s')\,\mathrm{dR(s, s')}\right)\right). \tag{10}$$

Note how the functional in (10) is the probabilistic analogue for the qualitative functional that characterizes the meaning of the temporal operator "Until" as the fixed point

$$p\,\mathrm{U}\,q = q \vee (p \wedge \mathrm{X}\,(p\,\mathrm{U}\,q)) \tag{11}$$

of linear-time temporal path formulas. We need to show that $\mathsf{M}(S, \Sigma)$ is an ω-dcpo and that $F(\phi_1, \phi_2)$, as defined in (10), is well defined.

Proposition 26. (1) *For any measure space (S, Σ), the pair $(\mathsf{M}(S, \Sigma), \leqslant)$ is an ω-dcpo with point-wise suprema and bottom element $\lambda s'.0$.*

(2) *For all ϕ_1, ϕ_2 of PCTL, the function $F(\phi_1, \phi_2)$ is well defined, monotone, and ω-continuous whenever $[\![\ \phi_1\ ]\!]$ and $[\![\ \phi_2\ ]\!]$ are in Σ.*

Proof. (1) The function $\lambda s'.0$ is constant and so in $\mathsf{M}(S, \Sigma)$, and the bottom element of $\mathsf{M}(S, \Sigma)$ as $\lambda s'.0 \leqslant f$ for all $f \in \mathsf{M}(S, \Sigma)$. A countable chain $(f_n)_{n\in\mathbb{N}}$ in $\mathsf{M}(S, \Sigma)$ is an increasing sequence of non-negative measurable functions and so their point-wise supremum is measurable again and the supremum of that chain in $\mathsf{M}(S, \Sigma)$.

(2) From $[\![\ \phi_1\ ]\!], [\![\ \phi_2\ ]\!] \in \Sigma$ we infer that $\chi_{[\![\phi_1]\!]}$ and $\chi_{[\![\phi_2]\!]}$ are in $\mathsf{M}(S, \Sigma)$. As maxima and minima of measurable functions are measurable it suffices to show that, for all $f \in \mathsf{M}(S, \Sigma)$, the function $\lambda s. \int f(s')\,\mathrm{d}R(s, s')$ is total and in $\mathsf{M}(S, \Sigma)$. Said function is total since all such f are non-negative and bounded by 1, so all integrals $\int f(s')\,\mathrm{d}R(s, s')$ exist.

As for measurability, let $f \in \mathsf{M}(S, \Sigma)$ first be a step function, a linear combination $\sum_i \beta_i \cdot \chi_{B_i}$ of finitely many characteristic functions of measurable sets $B_i \in \Sigma$ with $\beta_i \in [0, 1]$. Then $\lambda s. \int f(s')\,\mathrm{d}R(s, s') = \lambda s. \sum_i \beta_i \cdot R(s, B_i)$ is measurable since each $\lambda s. R(s, B_i)$ is, for R is a stochastic kernel. Since f is non-negative and measurable, there is an increasing sequence $(f_n)_{n\in\mathbb{N}}$ of such non-negative step functions with $f = sup_n f_n$ (point-wise) and so

$sup_n \int f_n \,\mathrm{d}\mu = \int f \,\mathrm{d}\mu$ for all measures μ on (S, Σ), by general properties of integrals. Since limits are point-wise, $\lambda s. \int f(s') \,\mathrm{d}R(s, s')$ is $sup_n \lambda s. \int f_n(s') \,\mathrm{d}R(s, s')$ which is measurable as the limit of an increasing sequence of measurable functions. Hence $F(\phi_1, \phi_2)$ is well defined if $[\![\phi_1]\!]$ and $[\![\phi_2]\!]$ are in Σ.

As constant functions, max, and min are ω-continuous, it remains to show that $F: \mathsf{M}(S, \Sigma) \to \mathsf{M}(S, \Sigma)$ with $F(f) = \lambda s. \int f(s') \,\mathrm{d}R(s, s')$ is ω-continuous. The latter is secured in the same manner in which we showed that F maps into $\mathsf{M}(S, \Sigma)$, noting that the function F is monotone as $f \leqslant g$ implies $\int f \,\mathrm{d}\mu \leqslant \int g \,\mathrm{d}\mu$ for all measures μ. □

With this machinery in place, we can define the meaning of the temporal operator "Until." For a function $F: \mathsf{M}(S, \Sigma) \to \mathsf{M}(S, \Sigma)$ we set

$$F^0 = \lambda f. f,$$
$$F^{n+1} = F \circ F^n \quad (n \in \mathbb{N}),$$

so that $F^n(f)$ has the effect of the $n$fold application of F to f.

Definition 27. Let $[\![\phi_1]\!]$ and $[\![\phi_2]\!]$ be in Σ. If ϕ_1 and ϕ_2 are determined by context, we write

$$\lambda s. P(s, k) = F(\phi_1, \phi_2)^{k+1}(\lambda s'.0),$$
$$\lambda s. P(s, \infty) = sup_{k \in \mathbb{N}} F(\phi_1, \phi_2)^{k+1}(\lambda s'.0)\,.$$

For $k \in \mathbb{N} \cup \{\infty\}$ we set

$$[\![[\phi_1 \,\mathsf{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}]\!] = \{s \in S \mid P(s, k) \sqsupseteq p\}\,. \tag{12}$$

As a sanity check we compute $\lambda s. P(s, 0)$, which is defined as the function $\max(\chi_{[\![\phi_2]\!]}, \min(\chi_{[\![\phi_1]\!]}, \lambda s. \int (\lambda s'.0) \,\mathrm{d}R(s, s'))) = \max(\chi_{[\![\phi_2]\!]}, \min(\chi_{[\![\phi_1]\!]}, \lambda s.0)) = \chi_{[\![\phi_2]\!]}$, rendering the intended meaning for $k = 0$. The unfoldings of the function $F(\phi_1, \phi_2)$, starting at the bottom element $\lambda s'.0$, correspond to the recursive computation of the numbers $P(s, k)$ in [22], whereas the least fixed point of $F(\phi_1, \phi_2)$ corresponds to the function $\lambda s. P(s, \infty)$ for the numbers $P(s, \infty)$ of loc. cit. In particular, our concrete semantics coincides with the PCTL semantics of loc. cit. on all discrete finite-state labelled Markov chains.

Example 28. For the model in Fig. 1 we compute $[\![[q_1 \vee \neg q_2 \,\mathsf{U}^{\leqslant 3}\, \neg q_2]_{\geqslant 0.80}]\!]$. First, $[\![q_1 \vee \neg q_2]\!] = S \setminus \{s_3\}$ and $[\![\neg q_2]\!] = \{s_0, s_1, s_d\}$. We write functions $\lambda s. P(s, k)$ as vectors $(v_0, v_1, v_2, v_3, v_d)$ and so obtain $\lambda s. P(s, 0) = (1, 1, 0, 0, 1)$, $\lambda s. P(s, 1) = (1, 1, 0.64 \cdot 0 + 0.36 \cdot 1, 0.5 \cdot 1 + 0.5 \cdot 0, 1) = (1, 1, 0.36, 0.5, 1)$, and similarly $\lambda s. P(s, 2) = (1, 1, 0.68, 0.68, 1)$ and $\lambda s. P(s, 3) = (1, 1, 0.7952, 0.84, 1)$. Thus, $[\![[q_1 \vee \neg q_2 \,\mathsf{U}^{\leqslant 3}\, \neg q_2]_{\geqslant 0.80}]\!] = S \setminus \{s_2\}$.

Proposition 29. *For all ϕ of PCTL, $[\![\phi]\!]$ is well defined and in Σ.*

Proof. We use structural induction on ϕ, where all cases except the one for the temporal operator "Until" are argued as in the proof of Proposition 4. For formulas of the form $[\phi_1 \,\mathsf{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}$ with $k \in \mathbb{N} \cup \{\infty\}$ we use induction on ϕ_1 and ϕ_2, the equation in (12),

and the fact that the least fixed point $\lambda s.P(s,\infty)$ of $F(\phi_1,\phi_2)$ and all its finite unfoldings $\lambda s.P(s,n)$ with $n \in \mathbb{N}$ are in $\mathsf{M}(S,\Sigma)$. $\square$

6. Abstract semantics of PCTL

We extend the abstract semantics $[\![\ \phi\ ]\!]^m$ from PPML to PCTL and prove its soundness. The semantics $[\![\ [\phi\, \mathrm{U}^{\leqslant k}\, \phi]_{\sqsupseteq p}\ ]\!]^m$ uses weighted sums of abstract measures of maximal sets for which the argument function for the next-state transformer has the same value. This manner of summation is as close as one can get to an "integration" of non-additive monotone set functions. Our soundness results also apply if we re-interpret $[\![\ [\mathrm{X}\phi]_{\sqsupseteq p}\ ]\!]^m$ from Definition 11 in this manner.

Definition 30. (1) For each $t \in \hat{S}$, ϕ_1, ϕ_2 of PCTL, and $m \in \{a,c\}$ we define a function $F(\phi_1,\phi_2,m)\colon \mathsf{M}(\hat{S},\mathbb{P}(\hat{S})) \to \mathsf{M}(\hat{S},\mathbb{P}(\hat{S}))$ by

$$F(\phi_1,\phi_2,m)(f) = \max\left(\chi_{[\![\phi_2]\!]^m}, \min\left(\chi_{[\![\phi_1]\!]^m}, \lambda t.\sum_{i=1}^{k} \hat{R}^m(t,B_i)\cdot r_i\right)\right) \tag{13}$$

where we use $\{f(t') \mid t' \in \hat{S}\} = \{r_1, r_2, \ldots, r_k\}$, $B_i = f^{-1}(r_i)$, and $r_i \neq r_j$ whenever $i \neq j$.

(2) Let $m \in \{a,c\}$. If ϕ_1 and ϕ_2 are determined by context, we denote

$$\lambda t.P(t,k,m) = F(\phi_1,\phi_2,m)^{k+1}(\lambda t'.0),$$
$$\lambda t.P(t,\infty,m) = sup_{k\in\mathbb{N}} F(\phi_1,\phi_2,m)^{k+1}(\lambda t'.0)\,.$$

For $k \in \mathbb{N} \cup \{\infty\}$ we set

$$[\![\ [\phi_1\, \mathrm{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}\ ]\!]^m = \{t \in \hat{S} \mid P(t,k,m) \sqsupseteq p\}\,. \tag{14}$$

Remark 31. If we use the finite measures $\lambda B.\tilde{R}^m(t,B)$ for the semantics of "next" in the meaning for formulas containing the temporal operator "Until" in (11) and (13) and formulas $[\mathrm{X}\phi]_{\sqsupseteq p}$, we extend the approximative semantics $[\![\ \phi\ ]\!]^{\tilde{m}}$ to full PCTL and have $[\![\ \phi\ ]\!]^{\tilde{a}} \subseteq [\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]^c \subseteq [\![\ \phi\ ]\!]^{\tilde{c}}$ for all ϕ of PCTL. Therefore, $[\![\ \phi\ ]\!]^{\tilde{m}}$ soundly abstracts $[\![\ \phi\ ]\!]^m$ and so the former is sound whenever the latter is.

The soundness proof for PCTL reduces to establishing a set of inequalities.

Lemma 32. *For all* $\phi \in \mathrm{PCTL}$, $\rho.[\![\ \phi\ ]\!]^a \subseteq [\![\ \phi\ ]\!]$ *and* $[\![\ \phi\ ]\!].\rho \subseteq [\![\ \phi\ ]\!]^c$ *if*

$$\forall \phi_1,\phi_2 \in \mathrm{PCTL}\ \forall s\rho t\ \forall k \in \mathbb{N}\colon P(t,k,a) \leqslant P(s,k) \leqslant P(t,k,c)\,. \tag{15}$$

Proof. By Theorem 12 and induction, it suffices to show the soundness for $[\![\ [\phi_1\, \mathrm{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}\ ]\!]^m$ with $k \in \mathbb{N} \cup \{\infty\}$ by induction on ϕ_1 and ϕ_2.

- For $k \in \mathbb{N}$ let $s\rho t$.
  - Given $s \in [\![\ [\phi_1\, \mathrm{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}\ ]\!]$, we have $P(s,k) \sqsupseteq p$. By (15), we get $P(t,k,c) \geqslant P(s,k) \sqsupseteq p$ and so $P(t,k,c) \sqsupseteq p$, i.e. $t \in [\![\ [\phi_1\, \mathrm{U}^{\leqslant k}\, \phi_2]_{\sqsupseteq p}\ ]\!]^c$ by (14).

- Let $t \in [\![[\phi_1 \, \mathrm{U}^{\leqslant k} \, \phi_2]_{\sqsupseteq p}]\!]^a$. So $P(t,k,a) \sqsupseteq p$. By (15), $P(s,k) \geqslant P(t,k,a) \sqsupseteq p$ and so $P(s,k) \sqsupseteq p$ which, by (12), means $s \in [\![[\phi_1 \, \mathrm{U}^{\leqslant k} \, \phi_2]_{\sqsupseteq p}]\!]$.

- For $k = \infty$ let $s\rho t$. Given $s \in [\![[\phi_1 \, \mathrm{U}^{\leqslant \infty} \, \phi_2]_{\sqsupseteq p}]\!]$, we have $sup_{n\in\mathbb{N}} P(s,n) \sqsupseteq p$. By (15), we get $P(t,\infty,c) = sup_{n\in\mathbb{N}} P(t,n,c) \geqslant sup_{n\in\mathbb{N}} P(s,n) \sqsupseteq p$ and so $P(t,\infty,c) \sqsupseteq p$, i.e. $t \in [\![[\phi_1 \, \mathrm{U}^{\leqslant \infty} \, \phi_2]_{\sqsupseteq p}]\!]^c$ by (14). One shows "$t \in [\![[\phi_1 \, \mathrm{U}^{\leqslant \infty} \, \phi_2]_{\sqsupseteq p}]\!]^a$ implies $s \in [\![[\phi_1 \, \mathrm{U}^{\leqslant \infty} \, \phi_2]_{\sqsupseteq p}]\!]$" in a dual manner. □

Whenever ρ is induced by a partition with measurable equivalence classes, we can secure the inequalities in (15).

Theorem 33. *Let $\{\rho.\{t\} \mid t \in \hat{S}\} \subseteq \Sigma$ be a partition of S. Then $\rho.[\![\phi]\!]^a \subseteq [\![\phi]\!]$ and $[\![\phi]\!].\rho \subseteq [\![\phi]\!]^c$ for all ϕ of PCTL.*

Proof. We assume that $\rho.[\![\phi_i]\!]^a \subseteq [\![\phi_i]\!]$ and $[\![\phi_i]\!].\rho \subseteq [\![\phi_i]\!]^c$ hold for all $i = 1, 2$. By induction and Lemma 32 it suffices to show (15). First, we prove $P(s,k) \leqslant P(t,k,c)$ for all $s\rho t$ by simultaneous induction on $k \in \mathbb{N}$.

- For $k = 0$, we already saw that $\lambda s.P(s,0) = F(\phi_1,\phi_2)(\lambda s'.0) = \chi_{[\![\phi_2]\!]}$. Similarly, $\lambda t.P(t,0,c) = \chi_{[\![\phi_2]\!]^c}$. If $P(s,0) = 0$ there is nothing to show. Otherwise, $P(s,0)$ equals 1 and so $s \in [\![\phi_2]\!]$ which, by induction on ϕ_2, renders $t \in [\![\phi_2]\!]^c$ and so $P(t,0,c) = 1$.
- If $P(s',k) \leqslant P(t',k,c)$ for all $s'\rho t'$, we show $P(s,k+1) \leqslant P(t,k+1,c)$.
  - If $s \in S \setminus ([\![\phi_1]\!] \cup [\![\phi_2]\!])$, then $P(s,k+1) = 0 \leqslant P(t,k+1,c)$.
  - If $s \in [\![\phi_2]\!]$, we can argue similarly to the case of $k = 0$.
  - Otherwise, we have $s \in [\![\phi_1]\!] \setminus [\![\phi_2]\!]$ and so

$$P(s,k+1) = \int P(s',k) dR(s,s') \,. \tag{16}$$

Now $s \in [\![\phi_1]\!]$ and induction on ϕ_1 render $t \in [\![\phi_1]\!]^c$. If $t \in [\![\phi_2]\!]^c$ as well, $P(t,k+1,c) = 1$ and so there is nothing to show. Otherwise, $t \in [\![\phi_1]\!]^c \setminus [\![\phi_2]\!]^c$ and therefore

$$P(t,k+1,c) = \sum_{i=1}^{k} \hat{R}^c(t,B_i) \cdot r_i \,, \tag{17}$$

where we use $\{P(t',k,c) \mid t' \in \hat{S}\} = \{r_1, r_2, \ldots, r_k\}$, $B_i = \{t' \in \hat{S} \mid P(t',k,c) = r_i\}$, and $r_i \neq r_j$ whenever $i \neq j$. By assumption, each $\rho.B_i$ is in Σ and so $\int_{\rho.B_i} f \mathrm{d}\mu = \int f \cdot \chi_{\rho.B_i} \mathrm{d}\mu$ exists for all measures μ since $\int f \, \mathrm{d}\mu$ exists. Therefore

$$\begin{aligned} P(s,k+1) &= \int P(s',k) \, \mathrm{d}R(s,s') \quad \text{by (16)} \\ &\leqslant \sum_{i=1}^{k} \int_{\rho.B_i} P(s',k) \, \mathrm{d}R(s,s') \quad \text{as } \bigcup_i \rho.B_i = S \\ &\leqslant \sum_{i=1}^{k} \int_{\rho.B_i} r_i \cdot \mathrm{d}R(s,s') \quad \text{by induction on } k \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{k} \left(\int_{\rho.B_i} \mathrm{dR(s, s')} \right) \cdot r_i \quad \text{moving a scalar} \\
&= \sum_{i=1}^{k} R(s, \rho.B_i) \cdot r_i \quad \text{as } \rho.B_i \in \Sigma \\
&= \sum_{i=1}^{k} R(s, \rho.B_i)_* \cdot r_i \quad \text{as } \rho.B_i \in \Sigma \\
&\leqslant \sum_{i=1}^{k} sup\{R(\bar{s}, \rho.B_i)_* \mid \bar{s}\rho t\} \cdot r_i \quad \text{as } s\rho t \\
&= \sum_{i=1}^{k} \hat{R}^c(t, B_i) \cdot r_i \quad \text{by definition of } \hat{R}^c \\
&= P(t, k+1, c) \quad \text{by (17) and (13)}.
\end{aligned}
$$

Second, we prove $P(t, k, a) \leqslant P(s, k)$ for all $s\rho t$ by simultaneous induction on $k \in \mathbb{N}$. This direction, unlike the previous one, relies on the fact that $\{\rho.\{t'\} \mid t' \in \hat{S}\} \subseteq \Sigma$ is a partition of S. Therefore $\{\rho.B_i \mid i = 1, 2, \ldots, k\}$, with the B_i and r_i defined and used in the inductive case below, is also a partition of S as $\bigcup_i \rho.B_i = S$ and $B_i \cap B_j = \{\}$ whenever $i \neq j$. Reasoned dually to the arguments for $P(s, k) \leqslant P(t, k, c)$, we may assume (16) and

$$
P(t, k+1, a) = \sum_{i=1}^{k} \hat{R}^a(t, B_i) \cdot r_i, \tag{18}
$$

where now $\{P(t', k, a) \mid t' \in \hat{S}\} = \{r_1, r_2, \ldots, r_k\}$, $B_i = \{t' \in \hat{S} \mid P(t', k, a) = r_i\}$, and $r_i \neq r_j$ whenever $i \neq j$. We compute

$$
\begin{aligned}
P(t, k+1, a) &= \sum_{i=1}^{k} \hat{R}^a(t, B_i) \cdot r_i \quad \text{by (18)} \\
&= \sum_{i=1}^{k} inf\{R(\bar{s}, \rho.B_i)^* \mid \bar{s}\rho t\} \cdot r_i \quad \text{by definition of } \hat{R}^a \\
&\leqslant \sum_{i=1}^{k} R(s, \rho.B_i)^* \cdot r_i \quad \text{as } s\rho t \\
&= \sum_{i=1}^{k} R(s, \rho.B_i) \cdot r_i \quad \text{as } \rho.B_i \in \Sigma \\
&= \sum_{i=1}^{k} \left(\int_{\rho.B_i} \mathrm{d}R(s, s') \right) \cdot r_i \quad \text{as } \rho.B_i \in \Sigma \\
&= \sum_{i=1}^{k} \int_{\rho.B_i} r_i \cdot \mathrm{d}R(s, s') \quad \text{moving a scalar} \\
&\leqslant \sum_{i=1}^{k} \int_{\rho.B_i} P(s', k)\, \mathrm{d}R(s, s') \quad \text{by induction on } k \\
&= \int P(s', k)\, \mathrm{d}R(s, s') \quad \text{as } \{\rho.B_i \mid i\} \text{ partition of } S \\
&= P(s, k+1) \quad \text{by (16)}. \qquad \square
\end{aligned}
$$

Example 34. We re-visit Example 28 and Remark 31 and illustrate the computation of $[\![[q_1 \vee \neg q_2 \,\mathrm{U}^{\leqslant 3}\, \neg q_2]_{\geqslant 0.80}]\!]^{\tilde{a}}$, where we write $\lambda t.P(t,k,\tilde{a})$ as a vector (v_0, v_1, v_d). Since $[\![q_1 \vee \neg q_2]\!]^{\tilde{a}} = [\![\neg q_2]\!]^{\tilde{a}} = \{t_0, t_d\}$ we have

$$\lambda t.P(t,0,\tilde{a})=(1,0,1), \qquad \lambda t.P(t,1,\tilde{a})=(1,0.36\cdot 1+0.5\cdot 0,1)=(1,0.36,1),$$
$$\lambda t.P(t,2,\tilde{a})=(1,0.54,1), \quad \lambda t.P(t,3,\tilde{a}) = (1,0.63,1)\,.$$

Note that this inability to verify the formula $[q_1 \vee \neg q_2 \,\mathrm{U}^{\leqslant 3}\, \neg q_2]_{\geqslant 0.80}$ at t_1 is built into the abstraction as $\rho.\{t_1\} = \{s_2, s_3\}$ identifies s_2 and s_3 but only the latter satisfies this formula containing the temporal operator "Until." In particular, this inability applies to the non-additive meaning $[\![[q_1 \vee \neg q_2 \,\mathrm{U}^{\leqslant 3}\, \neg q_2]_{\geqslant 0.80}]\!]^{a}$ as well. This suggests, as in the qualitative case, that abstractions need to be guided by formulas one wishes to check.

7. Related work

The work by Danos and Desharnais [12] is more general than ours in that it defines non-additive abstractions and their simulation without restricting to finite-state systems, develops the appropriate category-theoretic framework for these notions, and uses greatest fixed points for the approximation of cycles. The work in loc. cit. is less general than ours in that its logic does not support negation, its models either over- or under-approximate but do not combine these approximations, and the utility of its probabilistic logic in existing probabilistic model checkers is not directly apparent. The models of loc. cit. are event-based, ours are state-based.

Danos et al. [13] synthesize approximants by taking conditional averages of transition probabilities over equivalence classes that partition a state space. This approach preserves additivity of abstract measures, sits in between the over- and under-approximation of [12], reduces to taking probabilistic averages in finite-state systems, and marries well with the approximation of infinite-state systems in a metric for labelled Markov processes defined in [16].

Monniaux [33] proposes a formulaic language for the specification of trace properties of models that mix probabilistic choice and non-determinism. Two semantics, extending Kozen's duality [29] to the inclusion of non-determinism, are defined and their correspondence is proved.

D'Argenio et al. use probabilistic simulation based on a discrimination criterion in [14] to soundly abstract Markov decision processes with respect to the analysis of reachability properties.

In [19] Di Pierro et al. characterize probabilistic transition systems by means of linear operators on suitable vector spaces and reformulate notions of process equivalence as abstract linear operators so that one may identify processes whose abstractions differ by a specified amount, a measure of the effort needed in observing behavioral differences.

In [28] Jonsson and Larsen define probabilistic specifications, which are transition systems in which each transition is labelled with a set of allowed probabilities—a prominent example of such sets being closed intervals. They present a notion of refinement between probabilistic specifications and use extensions of methods from tree acceptors to give a complete decision procedure for containment of such specifications.

The work in [23] suggests the use of monotone measures for the abstraction of probabilistic systems and shares most objectives of the work presented in this paper but does not use stochastic kernels as a key ingredient of models: the transition relation R in loc. cit. has a different type which, unfortunately, results in the computation of very few "must"-transitions on abstractions.

In [24] computation tree logic is enriched with standard operators from hybrid logic [20], a three-valued abstraction for qualitative models is given, and a concrete semantics for PCTL with probabilistic hybrid operators is defined. Our results could easily be extended to the standard hybrid operators but an account thereof would make the paper too long and less focussed. The development of an abstraction for the probabilistic hybrid operators defined in [24], if possible at all, seems to be much more involved.

8. Future work

The contributions of this paper, apart from its semantics for PCTL over infinite-state systems, may seem somewhat straightforward as they combine the techniques of Danos and Desharnais [12] with those of three-valued abstraction in model checking [5,6,9,10,21]. But the presence of negation in PPML reveals that abstractions need to satisfy certain coherence conditions, which we identified in (5) and (6), to ensure the existence of optimal abstractions for finitely many formulas of PPML.

One could also develop such an abstraction approach for formulas without thresholds such that meanings are no longer Boolean values but values in $[0, 1]$, as done in [27] for the modal mu-calculus. In [25] it is shown that these two different approaches (probabilistic logic with thresholds and Boolean meanings vs. probabilistic logic without thresholds and meanings in $[0, 1]$) are related by an abstraction formalism.

In software verification one is often not interested in optimality results but in good abstract-and-refine methodologies [2]. But a refinement of an abstract model is driven by a counterexample and probabilistic model checkers currently offer little if any diagnostics that could be used to that end. Maybe optimality results and the computation of optimal abstractions can be an alternative to such methodologies in probabilistic model checking.

Our optimality results were limited to PPML. Future work would have to determine for which PCTL formulas beyond PPML one can obtain optimal, abstract finite-state models. For example, Dams and Namjoshi have shown [11] that there is an infinite-state Kripke structure M satisfying a CTL formula of the form "there is a path on which q_1 is true until q_2 is true" such that no finite-state, three-valued abstraction A of M satisfies that formula. We plan to find out whether this incompleteness result carries over to the two settings of this paper: abstractions through non-additive measures and abstractions through probabilistic measures only (e.g. obtained through $[\![\phi]\!]^{\tilde{m}}$). Of course, incompleteness for the latter would mean incompleteness for the former.

It is also beyond the scope of this paper to extract engineering principles for choosing effective abstractions, integrate such abstract checks within existing model checkers (e.g. PRISM [30]), specify a semantics of PCTL* for infinite-state systems, consider versions of PCTL that have intervals as thresholds, and study abstractions based on conditional expectations [13].

9. Conclusions

We presented a semantics for probabilistic computation tree logic on labelled Markov chains which extends the familiar one to *infinite-state* systems using basic tools from measure theory. For any left- and right-total relation between concrete and abstract states we constructed a three-valued model on abstract states, defined abstract semantics of probabilistic computation tree logic, and proved their soundness for the full probabilistic computation tree logic. For formulas containing the temporal operator "Until," this soundness required that the set of concrete states related to an abstract state is measurable. We showed that one may soundly abstract these abstract semantics with finite measures if one wishes to avoid the exponential penalty stemming from the representation of non-additive monotone set functions over the abstract state space. We also extended the results of Danos and Desharnais [12] to a probabilistic modal logic with full negation, requiring mild and always realizable conditions on state partitions or thresholds to show the existence of optimal finite-state approximants for finite sets of formulas of probabilistic propositional modal logic.

Acknowledgements

Radha Jagadeesan suggested to demote $[\![\phi]\!]^{\tilde{m}}$ to an example and to see the exponential overhead of computing $\lambda B.\hat{R}^m(t, B)$ as being similar to the overhead of computing abstract qualitative systems through the use of theorem provers (see e.g. [3]). Prakash Panangaden kindly suggested to look at the work by Danos and Desharnais [12], encouraged us to work on this material, helped in understanding why denotations for PCTL formulas are measurable, and alerted us to the fact that PPML with negation is more expressive than PPML without it. Iain Philipps suggested to consider, in future work, a variant of PCTL where thresholds are intervals rather than mere real numbers. Herbert Wiklicky pointed out that the domain theory needed in this paper is part of the folklore of measure theory. We thank the anonymous referees for making many suggestions on how to improve the presentation of this material and its context. Luca de Alfaro and Radha Jagadeesan are thanked for discussions on future work that helped with shaping Section 8.

References

[1] S. Abramsky, A. Jung, Domain Theory, in: S. Abramsky, D.M. Gabbay, T.S.E. Maibaum (Eds.), Handbook of Logic in Computer Science, Vol. 3, Oxford University Press, Oxford, 1994, pp. 1–168.

[2] T. Ball, B. Cook, S. Das, S.K. Rajamani, Refining approximations in software predicate abstraction, in: Proc. 10th Internat. Conf. on Tools and Algorithms for the Construction and Analysis of Systems, Barcelona, Spain, Lecture Notes in Computer Science, Vol. 2988, Springer, Berlin, 2004, pp. 388–403.

[3] T. Ball, A. Podelski, S.K. Rajamani, Boolean and Cartesian abstraction for model checking C programs, in: Proc. Seventh Internat. Conf. on Tools and Algorithms for the Construction and Analysis of Systems, Genova, Italy, Lecture Notes in Computer Science, Vol. 2031, Springer, Berlin, 2001, pp. 268–283.

[4] P. Billingsley, Probability and Measure, third ed., Wiley-Interscience, New York, 1995.

[5] G. Bruns, P. Godefroid, Model checking partial state spaces with 3-valued temporal logics, in: Proc. 11th Conf. on Computer Aided Verification, Trento, Italy, Lecture Notes in Computer Science, Vol. 1633, Springer, Berlin, 1999, pp. 274–287.

[6] G. Bruns, P. Godefroid, Generalized model checking: reasoning about partial state spaces, in: Proc. 11th Internat. Conf. on Concurrency Theory, University Park, Pennsylvania, Lecture Notes in Computer Science, Vol. 1877, Springer, Berlin, 2000, pp. 168–182.
[7] C. Courcoubetis, M. Yannakakis, The complexity of probabilistic verification, J. Assoc. Comput. Mach. 42 (4) (1995) 857–907.
[8] P. Cousot, R. Cousot, Abstract interpretation: a unified lattice model for static analysis of programs, in: Proc. Fourth ACM Symposium on Principles of Programming Languages, Los Angeles, California, ACM Press, New York, 1977, pp. 238–252.
[9] D. Dams, Abstract interpretation and partition refinement for model checking, Ph.D. Thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.
[10] D. Dams, R. Gerth, O. Grumberg, Abstract interpretation of reactive systems, ACM Trans. Programming Languages & Systems 19 (2) (1997) 253–291.
[11] D. Dams, K. Namjoshi, The existence of finite abstractions for branching time model checking, in: Proc. 19th Annu. IEEE Symp. on Logic in Computer Science, 13–17 July, Turku, Finland, IEEE Computer Society Press, Silver Springs, MD, 2004, pp. 335–344.
[12] V. Danos, J. Desharnais, Labelled Markov processes: stronger and faster approximations, in: Proc. 18th Annu. IEEE Symp. on Logic in Computer Science, Ottawa, Canada, IEEE Computer Society Press, Silver Springs, MD, 2003, pp. 341–350.
[13] V. Danos, J. Desharnais, P. Panangaden, Conditional expectations and the approximation of labelled Markov processes, in: R.M. Amadio, D. Lugiez (Eds.), Proc. 14th Internat. Conf. on Concurrency Theory, Marseille, France, Lecture Notes in Computer Science, Vol. 2761, Springer, Berlin, 2003, pp. 468–482.
[14] P.R. D'Argenio, B. Jeannet, H.E. Jensen, K.G. Larsen, Reachability analysis of probabilistic systems by successive refinements, in: L. de Alfaro, S. Gilmore (Eds.), PAPM-PROBMIV 2001, Aachen, Germany, Lecture Notes in Computer Science, Vol. 2165, Springer, Berlin, 2001, pp. 39–56.
[15] J. Desharnais, A. Edalat, P. Panangaden, Bisimulation for labelled Markov processes, J. Inform. Comput. 179 (2) (2002) 163–193.
[16] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Metrics for labelled Markov systems, in: J.C.M. Baeten, S. Mauw (Eds.), Proc. 10th Internat. Conf. on Concurrency Theory, Eindhoven, The Netherlands, Lecture Notes in Computer Science, Vol. 1664, Springer, Berlin, 1999, pp. 258–273.
[17] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Approximating labeled Markov processes, in: Proc. 15th Annu. IEEE Symp. on Logic in Computer Science, Santa Barbara, California, IEEE Computer Society Press, Silver Springs, MD, 2000, pp. 95–106.
[18] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, The metric analogue of weak bisimulation for probabilistic processes, in: Proc. 17th Annu. IEEE Symp. on Logic in Computer Science, Copenhagen, Denmark, IEEE Computer Society Press, Silver Springs, MD, 2002, pp. 413–422.
[19] A. Di Pierro, C. Hankin, H. Wiklicky, Quantitative relations and approximate process equivalences, in: Proc. 14th Internat. Conf. on Concurrency Theory, Marseille, France, Lecture Notes in Computer Science, Vol. 2761, Springer, Berlin, 2003, pp. 508–522.
[20] M. Franceschet, M. de Rijke, Model checking for hybrid logics, in: Proc. Workshop on Methods for Modalities, INRIA Lorraine, Nancy, France, September 2003.
[21] P. Godefroid, M. Huth, R. Jagadeesan, Abstraction-based model checking using modal transition systems, in: Proc. 12th Internat. Conf. on Theory and Practice of Concurrency, BRICS Aalborg, Denmark, Lecture Notes in Computer Science, Vol. 2154, Springer, Berlin, 2001, pp. 426–440.
[22] H.A. Hansson, B. Jonsson, A logic for reasoning about time and reliability, Formal Aspects Comput. 6 (5) (1994) 512–535.
[23] M. Huth, Possibilistic and probabilistic abstraction-based model checking, in: H. Hermanns, R. Segala (Eds.), Proc. Second Joint Internat. Workshop PAPM-PROBMIV 2002, Copenhagen, Denmark, Lecture Notes in Computer Science, Vol. 2399, Springer, Berlin, 2002, pp. 115–134.
[24] M. Huth, Abstraction and probabilities for hybrid logics, in: A. Cerone, A. Di Pierro (Eds.), Proc. Second Workshop in Quantitative Aspects of Programming Languages, Electronic Notes in Theoretical Computer Science, Vol. 112, Barcelona, Spain, 2004, pp. 61–76.
[25] M. Huth, An abstraction framework for mixed non-deterministic and probabilistic systems, in: C. Baier et al. (Eds.), Validation of Stochastic Systems, A Guide to Current Research, Lecture Notes in Computer Science, Vol. 2925, Springer, Berlin, 2004, pp. 419–444.

[26] M. Huth, R. Jagadeesan, D.A. Schmidt, Modal transition systems: a foundation for three-valued program analysis, in: D. Sands (Ed.), Proc. 10th European Symp. on Programming, Genova, Italy, Springer, Berlin, 2001, pp. 155–169.
[27] M. Huth, M. Kwiatkowska, Quantitative analysis and model checking, in: Proc. 12th Annu. IEEE Symp. on Logic in Computer Science, Warsaw, Poland, IEEE Computer Society Press, Silver Springs, MD, 1997, pp. 111–122.
[28] B. Jonsson, K.G. Larsen, Specification and refinement of probabilistic processes, in: Sixth Annu. IEEE Symp. on Logic in Computer Science, Amsterdam, The Netherlands, IEEE Computer Society Press, Silver Springs, MD, 1991, pp. 266–277.
[29] D. Kozen, Semantics of probabilistic programs, Comput. & Syst. Sci. 22 (1981) 328–350.
[30] M. Kwiatkowska, Model checking for probability and time: from theory to practice, Invited paper in the 18th Annu. IEEE Symp. on Logic in Computer Science, Ottawa, Canada, IEEE Computer Society Press, Silver Springs, MD, 2003, pp. 351–360.
[31] K.G. Larsen, B. Thomsen, A modal process logic, in: Third Annu. IEEE Symp. on Logic in Computer Science, Edinburgh, Scotland, IEEE Computer Society Press, Silver Springs, MD, 1988, pp. 203–210.
[32] G. Markowsky, Chain-complete posets and directed sets with applications, Algebra Universalis 6 (1) (1976) 53–68.
[33] D. Monniaux, Abstract interpretation of programs as Markov decision processes, in: R. Cousot (Ed.), Proc. 10th Internat. Symp. on Static Analysis, San Diego, California, Lecture Notes in Computer Science, Vol. 2694, Springer, Berlin, 2003, pp. 237–254.
[34] D.A. Schmidt, Structure-preserving binary relations for program abstraction, in: T. Mogensen, D. Schmidt, I.H. Sudburough (Eds.), The Essence of Computation: Complexity, Analysis, Transformation, Lecture Notes in Computer Science, Vol. 2566, Springer, Berlin, 2002, pp. 245–265.